AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Cancelled).

2. (Previously Presented) The method of Claim 27 wherein said step of substituting said source identification indicia with anonymous identification indicia comprises generating said anonymous identification indicia by using a character string and a portion of said source identification indicia in a mathematical hash algorithm.

3. (Original) The method of Claim 2 wherein said step of generating said anonymous identification indicia is repeated each time a subsequent message from a particular source is received such that said anonymous identification indicia is consistent for each source.

4. (Currently Amended) The method of Claim 27 wherein said step of substituting said source identification indicia with anonymous identification indicia is performed at a secure location where ~~the~~ a data analysis entity can only gain access with assistance from the system operator or an agent thereof and wherein the secure location comprises a computer that is password-protected and wherein the system operator, or an agent thereof, does not have the password but the data analysis entity does have the password.

5. (Cancelled).

6. (Cancelled).

7. (Previously Presented) The method of Claim 27 further comprising the step of inserting cable system source data into said first decrypted message.

8. (Original) The method of Claim 7 wherein said source data comprises cable system network segment data.

9. (Original) The method of Claim 7 wherein said source data comprises cluster code data.

10. (Previously Presented) The method of Claim 27 wherein said source is a set top box.

11. (Previously Presented) The method of Claim 27 wherein said source is a cell phone.

12. (Previously Presented) The method of Claim 27 wherein said source is a personal digital assistant.

13. (Cancelled).

14. (Previously Presented) The system of Claim 28 wherein said means for generating anonymous identification indicia comprises a computer-readable medium having computer-executable instructions for using a character string and a portion of said source identification indicia in a mathematical hash algorithm to generate said anonymous identification indicia.

15. (Original) The system of Claim 14 wherein said means for generating anonymous identification indicia repeats the use of said mathematical hash algorithm each time a subsequent message from a particular source is received such that said anonymous identification indicia is consistent for each source.

16. (Original) The system of Claim 15 wherein said source is a set top box.

17. (Original) The system of Claim 15 wherein the source comprises a memory chip that permits said source to receive the television programming content and wherein said source is a cell phone.

18. (Original) The system of Claim 15 wherein the source comprises a memory chip that permits said source to receive the television programming content and wherein said source is a personal digital assistant.

19. (Currently Amended) The system of Claim 28 wherein said server is positioned at a secure location where ~~athe~~ data analysis entity can only gain access to said secure location with assistance from the system operator or agent thereof and wherein said means for generating anonymous identification indicia comprises a computer that is password-protected and wherein the system operator does not have the password but the data analysis entity does have the password.

20. (Cancelled).

21. (Cancelled).

22. (Original) The system of Claim 15 further comprising means for inserting cable system source data into said first decrypted message.

23. (Original) The method of Claim 22 wherein said source data comprises cable system network segment data.

24. (Original) The method of Claim 22 wherein said source data comprises cluster code data.

25. (not entered).

26. (not entered).

27. (Currently Amended) A method for obscuring ~~the~~ an identity of ~~the~~ a source of a message while allowing ~~the~~ content of the message~~, and subsequent messages,~~ issued from that source to be analyzed ~~by a data analysis entity~~, and wherein the source is coupled to a cable

television system operated by a system operator for receiving television programming content therefrom, said method comprising the steps of:

obscuring the content of the message from a system operator by encrypting the content of a message issued from the source to form a first message, said first message containing source identification indicia and wherein the system operator knows the identity of the source of said first message, said first message being transmitted upstream to a remote device on the cable television system;

decrypting said first message into a first decrypted message upon receipt of said first message by said remote device;

substituting said source identification indicia with anonymous identification indicia into said first decrypted message to form a second message, and wherein said anonymous identification indicia cannot be traced back to the source ~~by the data analysis entity~~; and

encrypting said ~~first decrypted message along with said anonymous identification indicia into a~~ second message and transmitting said second message to a location to be analyzed.

28. (Currently Amended) A system for obscuring ~~the~~ an identity of ~~the~~a source of a message while allowing ~~the~~ content of the message~~, and subsequent messages,~~ issued from that source to be analyzed by a message content analysis means ~~managed by a data analysis entity~~, said system comprising:

means for encrypting, ~~contained within the source,~~ said encrypting means encrypting the message content along with source identifier indicia in ~~the~~ an encrypted message; and

a server, said server comprising:

means for decrypting the encrypted message into a first decrypted message;

means for generating anonymous identification indicia and for substituting the source identifier indicia with said anonymous identification indicia to form a second ~~first decrypted~~ message having said anonymous identification indicia embedded therein, wherein said anonymous identification indicia ~~can be traced back to the source by a system operator of the cable television system but~~ cannot be traced back to the source ~~by the data analysis entity~~;

means for encrypting said second ~~first decrypted~~ message having said anonymous identification indicia embedded therein to form a second encrypted message having said anonymous identification indicia embedded therein; and

wherein said server transmits upstream said second encrypted message having said anonymous identification indicia to the message content analysis means.

29. (New) A method for obscuring an identity of a source of a message while allowing content of the message issued from that source to be analyzed by a data analysis entity, and

wherein the source is coupled to a cable television system operated by a system operator for receiving television programming content therefrom, said method comprising the steps of:

obscuring the content of the message from a system operator by encrypting the content of a message issued from the source to form a first message, said first message containing source identification indicia and wherein the system operator knows the identity of the source of said first message, said first message being transmitted upstream to a remote device on the cable television system;

decrypting said first message into a first decrypted message upon receipt of said first message by said remote device;

generating anonymous identification data upon receipt of said first message by said remote device;

substituting said source identification indicia with anonymous identification indicia, and wherein said anonymous identification indicia cannot be traced back to the source by the data analysis entity; and

encrypting said first decrypted message along with said anonymous identification indicia into a second message and transmitting said second message to a location to be analyzed.

30. (New) A system for obscuring an identity of a source of a message while allowing content of the message to be analyzed, said system comprising:

an encrypting device adapted to encrypt the message content along with source identifier indicia in an encrypted message; and

a server, said server comprising:

means for decrypting the encrypted message into a first decrypted message;

a generator adapted to generate anonymous identification indicia upon receipt of said encrypted message and to substitute the source identifier indicia with said anonymous identification indicia wherein said anonymous identification indicia cannot be traced back to the source by the data analysis entity;

an encryption device adapted to encrypt said first decrypted message having said anonymous identification indicia embedded therein to form a second encrypted message having said anonymous identification indicia embedded therein; and

wherein said server transmits upstream said second encrypted message having said anonymous identification indicia.